Amendments to the Specification:

Please replace the Abstract with the following amended Abstract:

The present invention discloses a digital signature scheme based on braid group conjugacy problem and a verifying method thereof, wherein ~~the~~ a signatory S selects three braids $x \in L B_m(l)$, $x' \in B_n(l)$, $a \in B_n(l)$, and considers braid pair(x', x) as a public key of *S*, braid *a* as a private key of *S*; Signatory S uses hash function *h* for a message M needing signature to get $y=h(M) \in B_n(l)$; generating a braid $b \in RB_{n-1-m}(l)$ randomly, then signing ~~the message~~ *M* with ~~the own private key~~ *a* and ~~the braid~~ *b* ~~generated randomly~~ to obtain $Sign(M)=a^{-1}by^{b-1}a$; a signature verifying party *V* obtains the public key of *S*, calculating the message *M* by employing ~~a system parameter~~ hash function *h*, obtaining the $y=h(M)$; judging whether *sign(M)* and *y*, *sign(M)x'* and *xy* are conjugate or not, ~~if not, *sign(M)* is an illegal signature, the verification fails;~~ if yes, *sign(M)* is a legal signature of message M; the present invention ~~avoids the problem of k-CSP in SCSS signature scheme of prior art, and improves the security of signature algorithm and~~ reduces the number of braids involved and the number for conjugacy decision without reducing security, thereby improving the operation efficiency of signature.

Please replace the paragraph beginning on page 4, lines 13-15, with the following amended paragraph:

Step 1f. judging whether $x^{'}$ belongs to the supper summit set *SSS(x)* and whether $l(x^{'}) \leq d$, if all conditions are yes, outputting$(x, x^{'})$ as public key, *a* as private key; if either of them is not, performing step 1e.

Please replace the paragraph on page 5, lines 7-10, with the following amended paragraph:

In this method, the form for obtaining public key of the signatory *S* in step 1 is an out-band form or the form of receiving public key transmitted from the signatory *S*; ~~Algorithm~~ Conjugacy

decision algorithm in braid groups *BCDA* is employed in judging whether *sign(M)* and *y* are conjugate or not in step 3 and whether *sign(M) x'* and *xy* are conjugate or not in step 4.